REMARKS

Applicants respectfully traverse the rejection of claim 20 as being anticipated by the Hurtado publication (2003/0105718).

In particular, note that claim 20 is directed to a storage engine having a firmware component including a block configured to "verify one or more digital signatures" to a host seeking access to content controlled by the storage engine. The firmware includes another block configured to generate a random number and transmit the random number to the host. (In that regard, claim 20 has been amended analogously as discussed in the previous response with regard to claim 1: no new matter is added). The host may then decrypt content by combining the random number with an encrypted content key it receives from the storage engine.

Note the advantages of the method recited in claim 1: the DRM (digital rights management) is controlled by the storage engine rather than a host. This is advantageous because hackers cannot obtain access to the workings of the data storage engine as they would for a typical host such as a PC. In contrast, the Hurtado reference is a conventional "host-based" DRM scheme. In that regard, the office action of 10-18-05 states that Hurtado discloses a block configured to transmit a session key to the host in paragraphs 18, 181, 185 and 206-215. But note that these paragraphs are directed to the generation at the clearing house (element 105) of a decryption key. See, e.g., paragraph 181. Indeed, consider the end user device in Hurtado (Figure 1D). As set forth in the abstract, this end user must establish a "secure connection with an authorization authority" to decrypt desired content. As such, this is a classic host-based DRM scheme. Whatever storage engine the user device contains is entirely passive: just a disk reader. It in no way generates a random number, transmits the random number to a host, etc. Instead, it is the clearing house in Hurtado that generates the decryption key. In sharp contrast, it is the storage engine in claim 20 that generates the random number that enables a connected host device to decrypt content it is accessing through the storage engine.

The Liu reference (USP 6,760,752) adds nothing further. The Liu reference is merely directed to secure transmission of data over a network (see, e.g., the abstract). Liu provides no teaching or suggestion to modify the conventional host-based DRM scheme in Hurtado into the advantageous storage-engine-based DRM provided by the storage engine of claim 20. Accordingly, claim 20 is patentable over the cited prior art.

Claim 1 is patentable for analogous reasons. The cited prior art provides no suggestion or teaching for the inventive acts of "generating a random number at the storage engine and encrypting the random number with a public key extracted from the certificate to form a session key and transmitting the session key to the host" and "receiving an encrypted content key from the storage engine and decrypting the content key using the session key to recover the content key." As discussed above, the Hurtado reference is a conventional host-based scheme. There is no suggestion or teaching of a storage engine in Hurtado that generates a random number and encrypts the random number with a public key to form a session key and that transmits the session key to the host. Instead, all Hurtado discloses is a user device receiving decryption information through a secure connection to a clearing house. That is host-based and thus vulnerable to hacking scheme. In contrast, all the DRM "intelligence" recited in claim 1 is retained in the storage engine – a user has no access to this DRM capability and thus cannot hack it. Note further that content on the media is encrypted according to a content key. Thus, the host needs the content key to gain access to the content. However, for additional security, the storage engine does not simply provide the content key to the host. Instead, the content key is encrypted using the secure session key. Thus, the host can only recover the content key using the secure session key. As such, the secure session key is not a content key but rather is a key to the content key.

Thus, claim 1 and its dependent claims 2, 5-14, and 16-18 is patentable over the Hurtado and Liu references. Claim 20 is patentable for analogous reasons as discussed previously.

CONCLUSION

For the above reasons, claims 1, 2, 5 – 14, 16 – 18, and 20 are now in a condition for allowance. Applicant therefore respectfully requests that a timely Notice of Allowance be issued in this case.

If there are any questions regarding this amendment, the Examiner is invited to call the undersigned at (949) 752-7040.

Certification of Facsimile Transmission
I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Jonathan Hallman — February 21, 2006
Date of Signature

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicants
Reg. No. 42,622
Tel.: (949) 752-7040